Criteria

- การตรวจประเมินตามแนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ (HAIT Plus) พ.ศ. 2567
- เกณฑ์ Co-CERT

ระดับความเสี่ยง	HAIT Plus	Co-CERT
สูง	บทที่ 6 การสร้างมาตรการตรวจสอบเฝ้าระวัง มาตรการเผชิญเหตุ แก้ไขเมื่อพบภัยคุกคามทางไซเบอร์ และการกู้คืนระบบ	ระบบ Backup ข้อมูล
สูง	บทที่ 5 การทำให้ระบบมีความแข็งแกร่ง	ระบบ Antivirus Software
สูง	บทที่ 3 การประกาศนโยบาย มาตรฐานการปฏิบัติงาน ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และการสร้างความตระหนักรู้	Access Control (Public และ Private)
สูง	บทที่ 3 การประกาศนโยบาย มาตรฐานการปฏิบัติงาน ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และการสร้างความตระหนักรู้	"Privileged Access Management (PAM)

ระดับความเสี่ยง	HAIT Plus	Co-CERT
ปานกลาง	บทที่ 6 การสร้างมาตรการตรวจสอบเฝ้าระวัง มาตรการเผชิญเหตุ แก้ไขเมื่อพบภัยคุกคามทางไซเบอร์ และการกู้คืนระบบ	Business Continuity Plan (BCP)
ปานกลาง	บทที่ 6 การสร้างมาตรการตรวจสอบเฝ้าระวัง มาตรการเผชิญเหตุ แก้ไขเมื่อพบภัยคุกคามทางไซเบอร์ และการกู้คืนระบบ	Disaster Recovery site (DR)
ปานกลาง	บทที่ 5 การทำให้ระบบมีความแข็งแกร่ง	OS Patching
ปานกลาง	บทที่ 3 การประกาศนโยบาย มาตรฐานการปฏิบัติงาน ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และการสร้างความตระหนักรู้	Multi-Factor Authentication (2FA)
ปานกลาง	บทที่ 5 การทำให้ระบบมีความแข็งแกร่ง	Web Application Firewall (WAF)
ปานกลาง	บทที่ 6 การสร้างมาตรการตรวจสอบเฝ้าระวัง มาตรการเผชิญเหตุ แก้ไขเมื่อพบภัยคุกคามทางไซเบอร์ และการกู้คืนระบบ	Log Management
ปานกลาง	บทที่ 6 การสร้างมาตรการตรวจสอบเฝ้าระวัง มาตรการเผชิญเหตุ แก้ไขเมื่อพบภัยคุกคามทางไซเบอร์ และการกู้คืนระบบ	Security Information & Event Management (SIEM): ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ
ปานกลาง	บทที่ 4 การจัดการความเสี่ยง	Vulnerability Assessment (VA Scan)

ระดับความเสี่ยง	HAIT Plus	Co-CERT
ต่ำ	บทที่ 5 การทำให้ระบบมีความแข็งแกร่ง	Software Update
ต่ำ	บทที่ 5 การทำให้ระบบมีความแข็งแกร่ง	Penetration Testing
-	บทที่ 7 การจัดทำรายงานและการดูแลรักษาระบบอย่างต่อเนื่อง	

Management

1. องค์กรมีการจัดตั้งคณะทำงานเพื่อดำเนินการให้เกิดความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาลหรือไม่
2. คณะทำงานประกอบด้วยผู้แทนจากหน่วยงานที่เกี่ยวข้องครบถ้วนหรือไม่

Policy

1. องค์กรมีการจัดทำแผนปฏิบัติการสร้างระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นในโรงพยาบาล รวมถึงมีการติดตามความก้าวหน้าของการดำเนินงานหรือไม่
2. แผนปฏิบัติการครอบคลุมกิจกรรมที่จำเป็นและมีการกำหนดระยะเวลาดำเนินการที่ชัดเจนหรือไม่
3. องค์กรมีนโยบายและแนวปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์หรือไม่

Backup

1. การสำรองข้อมูลจะต้องสำรองข้อมูลระบบ HIS หรือระบบสารสนเทศที่สำคัญของโรงพยาบาลเป็นอย่างน้อย โดยมีรายละเอียดดังนี้
2. องค์กรมีการสำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง และสามารถดูข้อมูลย้อนหลังได้ 7 วันเป็นอย่างน้อยหรือไม่
3. องค์กรมีการจัดเก็บ Backup โดยสำเนาข้อมูล 3 ชุด และใช้เทคโนโลยีในการจัดเก็บข้อมูลต่างกัน 2 ชุด และเก็บ Offsite/Cloud 1 ชุด หรือไม่
4. Backup ข้อมูลครอบคลุม OS ของระบบ HIS หรือ software HIS เป็นอย่างน้อยหรือไม่

Antivirus Software

1. องค์กรมีการติดตั้ง Next-gen Antivirus, EDR, หรือ XDR บนเครื่อง Server ทุกเครื่องหรือไม่
2. องค์กรมีการ update signature ของ Anitivirus ต่ามข้อ 1. ทุกวันหรือไม่
3. Antivirus Active ตลอดเวลาหรือไม่ และครอบคลุม OS ของระบบ HIS เป็นอย่างน้อยหรือไม่

Access Control (Public/Private)

1. องค์กรมีการใช้ Firewall หรืออุปกรณ์ควบคุมการเข้าถึงระบบสารสนเทศภายในเครือข่ายหรือไม่
2. องค์กรมีการกำหนด White list Port และไม่เปิด Port ที่มีความเสี่ยงโดนโจมตีหรือไม่
3. องค์กรมีการแบ่งโซน Network ระหว่าง Server และ Client หรือไม่
4. องค์กรมีการใช้ VPN ในการเข้าถึง Server แทนการใช้ผ่าน Public หรือไม่
5. องค์กรมีการ Block การใช้งาน International Traffic หากไม่จำเป็นหรือไม่
6. องค์กรมีการใช้ Terminal server ในการเข้าถึง Server แทนที่ใช้ Computer ต้นทางหรือไม่

Privileged Access Management (PAM)

องค์กรต้องมีการจัดการสิทธิพิเศษในการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยครอบคลุมระบบ HIS เป็นอย่างน้อย ซึ่งมีรายละเอียดดังนี้

1. องค์กรมีการ Disable Administrator/Root/Admin บนระบบเพื่อป้องกันการโจมตีประเภท Brute Force Password หรือไม่
2. องค์กรมี Policy เปลี่ยน Password อย่างน้อยทุก 3 เดือนหรือไม่
3. องค์กรมีการกำหนดการเข้าถึงระบบตามสิทธิและหน้าที่ที่ได้รับหรือไม่ (User Right Matrix)
4. องค์กรมีการทบทวนสิทธิผู้ใช้งานอย่างน้อยปีละ 1 ครั้งหรือไม่
5. องค์กรมีการตั้ง Password ให้ Complex ตามมาตรฐาน (10 ตัวอักษร ใหญ่ เล็ก อักขระพิเศษ) หรือไม่

Business Continuity Plan (BCP)

1. องค์กรมีการจัดทำรายงานขั้นตอนการดำเนินการแผนความต่อเนื่องทางธุรกิจ (แผน BCP) ที่ชัดเจน รวมถึงระยะเวลาและผู้เกี่ยวข้องหรือไม่
2. การทำ BCP ครอบคลุม OS ของระบบ HIS หรือ Software HIS เป็นอย่างน้อยหรือไม่
3. องค์กรมีการทดสอบ BCP อย่างน้อยปีละ 1 ครั้งหรือไม่

Disaster Recovery Site (DR)

องค์กรมีศูนย์สำรองข้อมูล (DR-site) ในกรณีฉุกเฉินที่ระบบหลักมีปัญหาและใช้งานไม่ได้หรือไม่ โดย DR-site ต้องมีระยะห่างจากศูนย์ข้อมูลหลักไม่น้อยกว่า 60 กม. หรือไม่

OS Patching

องค์กรมีการ update Security Patch สำหรับ OS ของระบบ HIS อย่างน้อยปีละ 1 ครั้งหรือทันทีหาก มี Critical patch หรือไม่

Multi-Factor Authentication (2FA)

1. องค์กรมีการใช้ 2FA สำหรับ Admin ในการเข้าถึงระบบต่างๆ (VPN Access, Network Device, Security Device, Hypervisor, OS) หรือไม่
2. องค์กรมีการใช้ 2FA ครอบคลุม OS ของระบบ HIS หรือ Software HIS เป็นอย่างน้อยหรือไม่

Web Application Firewall (WAF)

1. องค์กรมีการใช้ Web Application Firewall (WAF) เพื่อป้องกันการโจมตีเว็บไซต์ของโรงพยาบาลตามมาตรฐาน OWASP Top 10 หรือไม่
2. องค์กรมีการใช้ WAF ครอบคลุม OS ของระบบ HIS หรือ Software HIS เป็นอย่างน้อยหรือไม่

Log Management

องค์กรมีระบบจัดเก็บ Log อินเตอร์เน็ตและคอมพิวเตอร์ตาม พ.ร.บ. อย่างน้อย 90 วันหรือไม่

Security Information & Event Management (SIEM)

องค์กรมีระบบ Security Information & Event Management (SIEM) เพื่อนำมาวิเคราะห์พฤติกรรม Cyber Attack บนระบบที่ให้บริการในระดับ Infrastructure และ OS หรือไม่

Vulnerability Assessment (VA Scan)

1. องค์กรมีการตรวจสอบช่องโหว่ หรือทำ VA Scan โดยครอบคลุม OS ของระบบ HIS หรือ Software HIS เป็นอย่างน้อยหรือไม่
2. หากพบช่องโหว่จากการ Scan แล้วมีการสรุปเป็นรายงานเพื่อนำไปสู่กระบวนการพิจารณาปิดช่องโหว่หรือไม่

Software Update

องค์กรมีการ update Software ของระบบ HIS เป็นอย่างน้อยหรือไม่

Penetration Testing

1. องค์กรมีการทดสอบเจาะระบบ หรือทำ Penetration Test อย่างน้อยปีละ 1 ครั้งหรือไม่
2. มีการสรุปผลการทดสอบเป็นรายงานเพื่อพิจารณาปรับปรุงความปลอดภัยของระบบหรือไม่

Incident Response Plan

1. องค์กรมีแผนรับมือและแจ้งเหตุกรณีเกิดเหตุภัยคุกคามทางไซเบอร์หรือไม่
2. กรณีเกิดเหตุภัยคุกคามทางไซเบอร์ องค์กรมีการจัดทำรายงานเหตุการณ์และแนวทางแก้ไขหรือไม่

2

เสี่ยงสูง

ทำทันที

- 1.1 BACKUP
- 1.2 Antivirus Software
- 1.3 Access Control (Public และ Private)
- 1.4 Privileged Access Management (PAM)

3

เสี่ยงกลาง

ควรต้องทำ

- 2.1 Business Continuity Plan (BCP)
- 2.2 Disaster Recovery Site (DR)
- 2.3 OS Patching
- 2.4 Multi-Factor Authentication
- 2.5 Web Application Firewall
- 2.6 Log Management
- 2.7 Secruity Information & Event Mnt
- 2.8 Vulnerbility Assessment

4

เสี่ยงต่ำ

เพิ่มความมั่นคง

- 3.1 Software Update
- 3.2 Penetration Testing
- 3.3 Dashboard
- 3.4 Cybersecurity Operations Center (CSOC)